

Serial No. 10/664,663

RECEIVED  
CENTRAL FAX CENTER  
SEP 17 2007

### LISTING OF THE CLAIMS

1       1. (Currently Amended) A method for protecting data  
2       generated by a keyboard, comprising the steps of:  
3              reading data from a keypad of the keyboard;  
4              reading an encryption seed from a device reader  
5       directly connected to the keyboard;  
6              encrypting the read data using the encryption seed;  
7       and  
8              directly transmitting the encrypted data from the  
9       keyboard to a computer wherein the encrypted data is not  
10      transmitted via the device reader to the computer and the  
11      computer and the device reader are different devices.

1       2. (Original) The method of claim 1 further comprises  
2       the steps of receiving the transmitted encrypted data by the  
3       computer; and  
4              decrypting the received encrypted data by the  
5       computer.

1       3. (Original) The method of claim 1 wherein the step  
2       of transmitting comprises the step of using a wireless link over  
3       which the encrypted data is transmitted.

Serial No. 10/664,663

1           4. (Canceled)

1           5. (Canceled)

1           6. (Canceled)

1           7. (Previously Amended) The method of claim 1  
2       wherein the step of reading the encryption seed comprises the  
3       step of enabling the device reader with a personal identification  
4       number.

1           8. (Canceled)

1           9. (Currently Amended) A method for protecting data  
2       generated by a keyboard, comprising the steps of:  
3           generating a start signal by at least one of a special  
4       key on keyboard a keypad of the keyboard or multi-actuation of  
5       a number of keys on the keypad;  
6           reading data from [a] the keypad of the keyboard  
7       following generation of the start signal wherein the read data  
8       and the start signal are distinct;  
9           encrypting the read data in response to the start  
10      signal; and  
11       transmitting the encrypted data from the keyboard to a  
12      computer;  
13       receiving a unique stop signal from the keypad;

Serial No. 10/664,663

14        stopping the encryption of the read data and  
15        transmission of the encrypted data from the keyboard to the  
16        computer in response to the stop signal.

1            10. (Canceled)

1            11. (Currently Amended) The method of claim 10 9  
2        wherein the step of receiving the stop signal comprises the step  
3        of generating the stop signal by at least one of a special key on  
4        keyboard or multi-actuation of a number of keys on the keypad.

1            12. (Canceled)

1            13. (Canceled)

1            14. (Canceled)

1            15. (Canceled)

1            16. (Canceled)

1            17. (Canceled)

1            18. (Canceled)

1            19. (Canceled)

Serial No. 10/664,663

1 20. (Canceled)

1 21. (Canceled)

1 22. (Canceled)

1 23. (Canceled)

1 24. (Canceled)

1 25. (Canceled)

1 26. (Currently Amended) A keyboard for encrypting  
2 data before transmission to a computer directly connected to  
3 the keyboard via a link, comprising:

4 an interface connected to the link;

5 a memory;

6 a keypad for generating the data;

7 a device reader interface for reading a directly  
8 connected device reader to obtain a seed for an encryption  
9 routine wherein the device reader and the computer are  
10 different devices;

11 a processor for encrypting using the seed from the  
12 device reader the generated data from the keypad by execution  
13 of the encryption routine stored in the memory; and

Serial No. 10/664,663

14                   directly transmitting the encrypted data to the  
15                   computer via the interface and link bypassing the device reader  
16                   and device interface.

1                   27. (Original) The keyboard of claim 26 wherein the  
2                   link is a wireless link.

1                   28. (Canceled)

1                   29. (Canceled)

1                   30. (Original) The keyboard of claim 26 comprises a  
2                   special key which when actuated causes the processor to at  
3                   least start executing the encryption routine or stop executing  
4                   the encryption routine.

1                   31. (Currently Amended) A processor-readable  
2                   medium for protecting data generated by a keyboard,  
3                   comprising processor-executable instructions configured for:  
4                   reading data from a keypad of the keyboard;  
5                   reading an encryption seed from a device reader  
6                   directly connected to the keyboard;  
7                   encrypting the read data using the encryption seed;  
8                   and  
9                   directly transmitting the encrypted data from the  
10                  keyboard to a computer wherein the encrypted data is not

Serial No. 10/664,663

11    transmitted via the device reader to the computer and the  
12    computer and the device reader are different devices.

1            32. (Original) The processor-readable medium of  
2    claim 31 wherein the transmitting comprises using a wireless  
3    link over which the encrypted data is transmitted.

1            33. (Canceled)

1            34. (Canceled)

1            35. (Canceled)

1            36. (Previously Amended) The processor-readable  
2    medium of claim 31 wherein the reading the encryption seed  
3    comprises enabling the device reader with a personal  
4    identification number.

1            37. (Canceled)

1            38. (Currently Amended) A processor-readable  
2    medium for protecting data generated by a keyboard,  
3    comprising processor-executable instructions configured for:  
4            generating a start signal by at least one of a special  
5    key on keyboard a keypad of the keyboard or multi-actuation of  
6    a number of keys on the keypad;

Serial No. 10/664,663

7 reading data from [a] the keypad of the keyboard  
8 following generation of the start signal wherein the read data  
9 and the start signal are distinct;  
10 encrypting the read data in response to the start  
11 signal; and  
12 transmitting the encrypted data from the keyboard to a  
13 computer;  
14 receiving a unique stop signal from the keypad;  
15 stopping the encryption of the read data and  
16 transmission of the encrypted data from the keyboard to the  
17 computer in response to the stop signal.

1 39. (Canceled)

1 40. (Currently Amended) The processor-readable  
2 medium of claim 39 38 wherein the stop signal generated by at  
3 least one of a special key on keyboard or multi-actuation of a  
4 number of keys on the keypad.

1 41. (Canceled)

1 42. (Canceled)

1 43. (Canceled)

1 44. (Canceled)

Serial No. 10/664,663

1 45. (Canceled)

1 46. (Canceled)

1 47. (Canceled)

1 48. (Canceled)